

OLD DOMINION UNIVERSITY
University Policies and Procedures

3512 - DATA CLASSIFICATION POLICY

Statement: Data is one of the University's most valuable resources and requires responsible and ethical use. The university relies heavily on its information technology and data to meet its educational, research, informational and operational needs. It is essential that university data be classified so that systems are protected from misuse and that both information technology and all data be maintained in a secure environment.

This policy outlines the extent to which the data classification standard should be followed, the responsibilities of the university community in relation to the standard, and provides guidelines for classifying the data.

The University Data Classification Standard shall:

1. be based on the federal laws and those of the Commonwealth of Virginia, and must abide by other regulatory restrictions not specifically covered by state and federal laws;
2. apply to all data created and maintained by all campuses (e.g. student, research, financial, payroll) except where superseded by grant or other contract or by federal copyright law;
3. include all University data regardless of the medium on which it resides (e.g., paper, fiche, electronic form on tape, cartridge, disk, CD-ROM) and regardless of form (e.g., text, graphic, video, voice);
4. apply to all authorized users of the Old Dominion University; and
5. comply with the applicable federal and state laws, which govern the privacy and confidentiality of data, including the Electronic Communications Act of 1986, and the Federal Rights and Privacy Act of 1974.

The President (or his designee) will appoint data custodians who are responsible for the day-to-day oversight of data as outlined below.

Data custodians are responsible for:

1. knowing and understanding the data for which they are responsible, and
2. evaluating and ensuring the data has been appropriately classified based on state and federal law, regulatory agency requirements and any contractual obligations; University regulations; and the confidentiality, criticality and sensitivity of data as listed below.

Data Classification Standard:

Five levels of data classification have been established.

1. Unclassified - data that does not fall into any of the other data classifications noted below. This data may be made generally available without specific Data Custodian approval;
2. Operation Use Only - data whose loss, corruption or unauthorized disclosure would not necessarily result in any business, financial or legal loss, but is made available to Data Custodian approved users only;
3. Private - data whose disclosure would not result in any business, financial or legal loss but involves issues of personal credibility, reputation, or other issues of personal privacy;
4. Restricted - data whose loss, corruption or unauthorized disclosure would tend to impair the business or research functions of the University, or result in business, financial, or legal loss;
5. Confidential - data whose loss, corruption or unauthorized disclosure would be a violation of federal or state laws/regulations or University contracts.

All data regardless of medium and/or form, will be identified as to its classification (i.e. Unclassified, Operational Use Only, Private, Restricted or Confidential).

Aggregates of data should be classified based upon the most secure classification level; in other words, when data of mixed classification exist in the same file, report or memorandum, the classification of the same file, report or memorandum should be of the highest level of classification).

Responsibility: Vice President for Administration and Finance

Authorization: James V. Koch, President

Date: July 1, 2000

Effective Date: July 1, 2000